



Der ECC-Brainpool veranstaltet am 8.4.2002 einen Workshop zu dem Thema

Alternative Public-Key-Algorithmen

Alle Mitglieder des ECC-Brainpool sind herzlich eingeladen, daran teilzunehmen. Auch andere Teilnehmer sind – nach Anmeldung und Bestätigung per E-Mail – willkommen. Die Veranstaltung ist kostenlos. Der Ort der Veranstaltung ist:

**Zentrum für IT-Sicherheit
Lise-Meitner-Allee 4
44780 Bochum**

Geplantes Programm:

- 10:00 Uhr: Begrüßung
- 10:10 Uhr: The XTR crypto system - Efficient arithmetic in $GF(p^6)$ (*K. Nguyen, Philips*)
- 10:45 Uhr: NICE-X - An IND-CCA2 Public-Key Cryptosystem with Fast Decryption using Quadratic Fields (*T. Takagi, TU Darmstadt*)
- 11:20 Uhr: Kaffeepause
- 11:35 Uhr: NTRU: Effiziente gitterbasierte Kryptographie (*C. Ludwig, TU Darmstadt*)
- 12:10 Uhr: Ein asymmetrisches Chiffrierverfahren von Niederreiter basierend auf der Dezimierung von Schieberegisterfolgen und das McEliece-Niederreiter-Sendrier-Kryptosystem (*R. Göttfert, Infineon*)
- 12:45 Uhr: Mittagspause
- 14:00 Uhr: Kryptographie mit Zopf-Gruppen (*M. Müller, SIT Rohde&Schwarz*)
- 14:35 Uhr: Hyperelliptische Kurven in der Kryptographie (*T. Lange, Uni Bochum*)
- 15:10 Uhr: Kaffeepause
- 15:25 Uhr: DL-Problem in endlichen Körpern mittlerer Charakteristik (*P. Mihalescu, Uni Paderborn, R. Avanzi, Uni Essen*)
- 16:00 Uhr: Multivariate Kryptographie (*M. Daum, P. Felke, Uni Bochum*)
- 16:35 Uhr: Kaffeepause
- 16:50 Uhr: Zahlkörperkryptographie (*A. Meyer, TU Darmstadt*)
- 17:25 Uhr: Optimal Extension Fields for ECC on Smart Cards (*C. Paar, Uni Bochum*)
- 18:00 Uhr: Ende der Veranstaltung

Um Anmeldung möglichst bis zum 3.4. wird gebeten. Anmeldungen gehen bitte per Email an info@ecc-brainpool.org. Wegen der Räumlichkeiten ist die Anzahl der Teilnehmer auf maximal 70 beschränkt.